5

2

5

CLAIMS

What is claimed is:

1. A method for tracking frequently occurring fail events that are detected during testcase simulation of a simulation model within a batch simulation farm wherein testcases are executed within respect to a simulation model on one or more simulation clients, said method comprising:

within an instrumentation server:

receiving fail event packets from said simulation clients, wherein said fail event packets contains an aggregate of detected occurrences of a specified fail event; and

monitoring the rate of occurrence of said specified fail event from received fail event packets to detect an excess rate of occurrence of said specified fail event.

2. The method of claim 1, further comprising:

within said instrumentation server:

maintaining a counter that specifies the rate of occurrences of said specified fail event;

reading said received aggregate fail event packet; and

list.

6

6

responsive to said aggregate fail event packet including a recorded

occurrence of said specified fail event, incrementing said counter. 7 3. The method of claim 2, further comprising decrementing said counter at a predetermined time interval such that a rate of occurrence of said specified fail event may be determined within said instrumentation server. 3 4. The method of claim 1, further comprising: within said instrumentation server: comparing the rate of occurrence of said specified fail event with a predetermined threshold rate; and responsive to the rate of occurrence of said specified fail event exceeding said predetermined threshold rate, adding said specified fail event to a fail event disable list. 5. The method of claim 4, further comprising: prior to testcase simulation of said simulation model within said one or more simulation clients: 3 retrieving said fail event disable list from said instrumentation server; and disabling fail events specified within said instrumentation event disable

4

5

instrumentation server:

6. The method of claim 1, wherein said monitoring the rate of occurrence of said 1 specified fail event is preceded by: 2 delivering an instrumentation eventlist from said simulation client to said 3 instrumentation server, wherein said eventlist contains instrumentation event information for said simulation model; and 5 within said instrumentation server: 6 computing a digital signature that uniquely identifies contents of said instrumentation eventlist as being associated with said simulation model; and responsive to receiving simulation data from said simulation client, utilizing said digital signature to associate said simulation data with said simulation model. 7. The method of claim 6, wherein said instrumentation server computes said digital signature utilizing a cyclic redundancy check algorithm, said method further comprising computing a digital signature within said simulation client utilizing said cyclic redundancy check algorithm. 8. The method of claim 7, wherein said monitoring the rate of occurrence of said specified fail event is preceded by: 2

responsive to receiving said aggregate fail event packet within said

comparing the digital signature contained in said aggregate

7

8

10

11

12

7

8

9

10

11

12

instrumentation packet with the digital signature computed by said instrumentation server to determine whether or not a match exists;

responsive the digital signature contained in said aggregate fail event packet matching the digital signature computed by said instrumentation server, processing said aggregate fail event packet within said instrumentation server; and

responsive to the digital signature contained in said aggregate instrumentation packet not matching the digital signature computed by said instrumentation server, discarding said aggregate fail event packet.

9. A system for tracking frequently occurring fail events that are detected during test case simulation of a simulation model within a batch simulation farm wherein testcases are executed within respect to a simulation model on one or more simulation clients, said system comprising:

an instrumentation server including processing means for:

receiving fail event packets from said simulation clients, wherein said fail event packets contains an aggregate of detected occurrences of a specified fail event; and

monitoring the rate of occurrence of said specified fail event from received fail event packets to detect an excess rate of occurrence of said specified fail event.

5

2

10. The system of claim 9, wherein said instrumentation server further comprises:
a counter that specifies the rate of occurrences of said specified fail event;
processing means for reading said received aggregate fail event packet; and

processing means responsive to said aggregate fail event packet including a recorded occurrence of said specified fail event for incrementing said counter.

- 11. The system of claim 10, further comprising processing means for decrementing said counter at a predetermined time interval such that a rate of occurrence of said specified fail event may be determined within said instrumentation server.
- 12. The system of claim 9, wherein said instrumentation server further comprises:

processing means for comparing the rate of occurrence of said specified fail event with a predetermined threshold rate; and

processing means responsive to the rate of occurrence of said specified fail event exceeding said predetermined threshold rate for adding said specified fail event to a fail event disable list.

13. The system of claim 12, further comprising:

processing means for retrieving said fail event disable list from said instrumentation server; and

5

l

2

3

4

1

3

4

ŀ

2

3

processing means for disabling fail events specified within said instrumentation event disable list.

14. The system of claim 9, further comprising:

processing means for delivering an instrumentation eventlist from said simulation client to said instrumentation server, wherein said eventlist contains instrumentation event information for said simulation model; and

within said instrumentation server:

processing means for computing a digital signature that uniquely identifies contents of said instrumentation eventlist as being associated with said simulation model; and

processing means responsive to receiving simulation data from said simulation client for utilizing said digital signature to associate said simulation data with said simulation model.

- 15. The system of claim 14, wherein said instrumentation server computes said digital signature utilizing a cyclic redundancy check algorithm, said system further comprising processing means for computing a digital signature within said simulation client utilizing said cyclic redundancy check algorithm.
- 16. The system of claim 15, further comprising:

processing means responsive to receiving said aggregate fail event packet within said instrumentation server for:

5

6

7

8

9

10

7

8

9

10

11

comparing the digital signature contained in said aggregate instrumentation packet with the digital signature computed by said instrumentation server to determine whether or not a match exists;

responsive the digital signature contained in said aggregate fail event packet matching the digital signature computed by said instrumentation server, processing said aggregate fail event packet within said instrumentation server; and

responsive to the digital signature contained in said aggregate instrumentation packet not matching the digital signature computed by said instrumentation server, discarding said aggregate fail event packet.

17. A computer program product for tracking frequently occurring fail events that are detected during test case simulation of a simulation model within a batch simulation farm wherein testcases are executed within respect to a simulation model on one or more simulation clients, said computer program product comprising:

program instruction means for receiving fail event packets from said simulation clients, wherein said fail event packets contains an aggregate of detected occurrences of a specified fail event; and

program instruction means for monitoring the rate of occurrence of said specified fail event from received fail event packets to detect an excess rate of occurrence of said specified fail event.

ł

2

3

5

3

4

5



18. The computer program product of claim 17, further comprising:

program instruction means for implementing a counter that specifies the rate of occurrences of said specified fail event;

program instruction means for reading said received aggregate fail event packet; and

program instruction means responsive to said aggregate fail event packet including a recorded occurrence of said specified fail event for incrementing said counter.

- 19. The computer program product of claim 18, further comprising program instruction means for decrementing said counter at a predetermined time interval such that a rate of occurrence of said specified fail event may be determined within said instrumentation server.
- 20. The computer program product of claim 17, further comprising:

program instruction means for comparing the rate of occurrence of said specified fail event with a predetermined threshold rate; and

program instruction means responsive to the rate of occurrence of said specified fail event exceeding said predetermined threshold rate for adding said specified fail event to a fail event disable list.

21. The computer program product of claim 20, further comprising:

4

5

2

3

4

1

2

3

program instruction means for retrieving said fail event disable list from said instrumentation server; and

program instruction means for disabling fail events specified within said instrumentation event disable list.

22. The computer program product of claim 17, further comprising:

program instruction means for delivering an instrumentation eventlist from said simulation client to said instrumentation server, wherein said eventlist contains instrumentation event information for said simulation model;

program instruction means for computing a digital signature that uniquely identifies contents of said instrumentation eventlist as being associated with said simulation model; and

program instruction means responsive to receiving simulation data from said simulation client for utilizing said digital signature to associate said simulation data with said simulation model.

- 23. The computer program product of claim 22, wherein said instrumentation server computes said digital signature utilizing a cyclic redundancy check algorithm, said computer program product further comprising program instruction means for computing a digital signature within said simulation client utilizing said cyclic redundancy check algorithm.
- 24. The computer program product of claim 23, further comprising:

program instruction means responsive to receiving said aggregate fail event packet within said instrumentation server for:



comparing the digital signature contained in said aggregate instrumentation packet with the digital signature computed by said instrumentation server to determine whether or not a match exists;

responsive the digital signature contained in said aggregate fail event packet matching the digital signature computed by said instrumentation server, processing said aggregate fail event packet within said instrumentation server; and

responsive to the digital signature contained in said aggregate instrumentation packet not matching the digital signature computed by said instrumentation server, discarding said aggregate fail event packet.